United States District Court
District of New Jersey

UNITED STATES OF AMERICA	:	**CRIMINAL COMPLAINT**
v.	:	
ALEXANDER BRAZHNIKOV aka "Alexandre Brajnikov," ABN UNIVERSAL, INC., ZOND-R, INC., TELECOM MULTIPLIERS, and ELECTRONICS CONSULTING	:	**Magistrate No. 14-3677**

I, Chetwyn M. Jones, the undersigned complainant being duly sworn, state the following is true and correct to the best of my knowledge and belief.

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached page and made a part hereof.

Chetwyn M. Jones, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,

June 26, 2014 at Newark, New Jersey
Date City and State

Honorable Mark Falk
United States Magistrate Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

ATTACHMENT A

Count One

Conspiracy to Commit Money Laundering

From in or about January 2008 through in or about June 2014, in Union County, in the District of New Jersey and elsewhere, the defendants ALEXANDER BRAZHNIKOV aka "Alexandre Brajnikov," ABN UNIVERSAL, INC., ZOND-R, INC., TELECOM MULTIPLIERS, and ELECTRONICS CONSULTING, together with others, did knowingly and intentionally conspire with each other and others to transmit and transfer monetary instruments and funds from a place outside the United States, to wit, Russia, to a place in the United States, to wit, New Jersey, with the intent to promote the carrying on of specified unlawful activity, namely the smuggling of electronics components from the United States contrary to Title 18, United States Code, Section 554(a), and contrary to Title 18, United States Code, Section 1956(a)(2)(A), in violation of Title 18, United States Code, Section 1956(h).

Count Two

Conspiracy to Smuggle Goods from the United States

From in or about January 2008 through in or about June 2014, in Union County, in the District of New Jersey and elsewhere, the defendants ALEXANDER BRAZHNIKOV aka "Alexandre Brajnikov," ABN UNIVERSAL, INC., ZOND-R, INC., TELECOM MULTIPLIERS, and ELECTRONICS CONSULTING, together with others, did knowingly and intentionally conspire and agree with each other and with others to fraudulently export and send from the United States merchandise, articles, and objects, including electronics components, contrary to Title 13, United States Code, Section 305, and to receive, conceal, buy, sell and in any manner facilitate the transportation, concealment, or sale of such merchandise, articles and objects, prior to exportation, knowing the same to be intended for exportation, contrary to Title 18, United States Code, Section 554(a).

In furtherance of the conspiracy and to effect its unlawful objects, the above-listed defendants and their co-conspirators committed and caused to be committed the overt acts, among others, in the District of New Jersey and elsewhere, as set forth in Attachment B below, in violation of Title 18, United States Code, Section 371.

ATTACHMENT B

I, Chetwyn M. Jones, am a Special Agent with the Federal Bureau of Investigation ("FBI"). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and other pertinent items of evidence. Where statements of others are related herein, they are related in substance and in part. Because this complaint is being submitted for a limited purpose of establishing probable cause to support the issuance of a complaint and arrest warrant, I have not necessarily included each and every fact that I know or that other law enforcement agents know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the day alleged.

The Defendants

1. The defendant ALEXANDER BRAZHNIKOV aka "Alexandre Brajnikov," is the owner, chief executive officer, and principal operator of the following privately held, New Jersey business entities: (a) defendant ABN UNIVERSAL, INC., a microelectronics export company formerly located in Carteret, NJ; (b) defendant ZOND-R, INC., a microelectronics export company with its principal place of business in Union, NJ; (c) defendant TELECOM MULTIPLIERS, a microelectronics export company with its principal place of business in Mountainside, NJ; and (d) defendant ELECTRONICS CONSULTING, INC., a microelectronics export company with its principal place of business in Manalapan, NJ (hereinafter, collectively, the "NJ Export Companies").

Summary of Investigation

2. Defendant ALEXANDER BRAZHNIKOV aka "Alexandre Brajnikov," (hereinafter, "Brazhnikov") and the defendant NJ Export Companies, together with others known and unknown (hereinafter, collectively, the "defendants"), are part of an illicit, sophisticated, international electronics procurement network that is designed to surreptitiously acquire large quantities of electronic components from United States manufactures and vendors, and to export those parts to Russia, on behalf of Russian business entities that are authorized to supply those parts to the Ministry of Defense of the Russian Federation, as well as the Federal Security Service of the Russian Federation (the "FSB"). Over approximately the last four years, this network has obtained and exported over $65 million worth of electronics from the United States to Russian business entities in violation of export control laws, as further described herein.

3. An investigation conducted by the FBI beginning in or about December 2012 has revealed that the defendants' Moscow-based conspirators are responsible for obtaining initial requests for quotes ("RFQs") for U.S. electronics components from various Russian entities, including licensed defense contractors. Those requests were then communicated by the Moscow-based conspirators either directly to U.S. vendors by

electronic means or by sending the requests to the defendants in the U.S. Using the NJ Export Companies, the defendants finalize the purchase and acquisition of the requested components from the various U.S.-based distributors. In order to make these purchases, however, the defendants conceal the true identity of the ultimate end-user[1] of the components in Russia. Upon receipt of the components at the NJ Export Companies' locations, defendant Brazhnikov and his co-conspirators re-packaged and prepared the parts for export to Russia via various shipping companies based in New York and New Jersey. In violation of U.S. export control laws, defendant Brazhnikov and his co-conspirators falsified the true value of the exported items on shipping documents in order to evade the legal requirement of filing an Electronic Export Information ("EEI") via the Automated Export System ("AES"),[2] thereby concealing their export activities from the United States.

4. In addition to falsifying the value of the parts they export, the defendants routinely and systematically concealed the true destination of the parts they were exporting by directing that the shipments be sent to various recipients and addresses in Russia which are controlled by the Moscow-based conspirators. Specifically, an exhaustive review of banking records, purchase invoices, and shipping documents recovered in this investigation has identified approximately 1,670 shipments directed by the defendants to locations in Russia over approximately the last four years. Significantly, all of the shipments sent to the various named recipients in Russia have been traced to a total of twelve unique addresses in Moscow. These addresses are all located within six miles of one another, and law enforcement agents have confirmed that none of the addresses hosts any entity that could be described as a manufacturer, distributor, dealer, or any entity actually affiliated with the business of acquiring, shipping or selling electronics components. In fact, several of the addresses have been identified as vacant apartments or storefronts. Additionally, of the remaining shipments identified during this

---

1 The U.S. Department of State ("DOS") and the U.S. Department of Commerce ("DOC") require that certain forms (*i.e.*, 'end-user agreements') be properly executed in connection with the export of controlled items. The DOS requires a completed form DSP-83 be included as a part of an application for authorization to export significant military equipment and classified equipment or data. *See*, 22 C.F.R. §§ 123.10(a), 124.10 and 125.7. The form DSP-83 must be completed by the appropriate foreign persons (e.g., consignee, end-user, government) and forwarded to the DOS through the U.S. person/entity making the application. The DOC requires that a completed form BIS-711 ("Statement by Ultimate Consignee and Purchaser") be included as part of an application for authorization to export certain controlled items, subject to the parameters of 15 C.F.R. §§ 748, et. seq.

2 Criminal penalties for unlawful export information activities as they pertain to EEI's (formerly known as Shipper's Export Declaration ("SED") forms) are prescribed by 13 U.S.C. § 305. Generally, a DOC Form 7525-V (referred to herein as an "SED Form") is required for all shipments sent to foreign countries regardless of the method of transportation, subject to certain restrictions. As it applies to the instant investigation, SED forms must be filed when: (i) an item requires an export license; (ii) is bound for an embargoed country; or (iii) the value of the item(s) is greater than $2,500 (U.S.). SED forms are electronically filed with the DOC through the Automated Export System ("AES").

timeframe that were initially addressed to recipients in Finland or Germany, law enforcement agents have traced the final destination of those shipments to one of the twelve known Moscow addresses. Based on these facts, and other information obtained during this investigation, law enforcement agents have concluded that each of the twelve addresses contained in the six mile radius in Moscow act as shell entities utilized by the defendants as part of their ongoing, illicit procurement of U.S. electronics components. The use by the defendants of these recipient shell entities indicates that the defendants systematically falsify the true end-user of the electronics components they obtain from U.S. vendors and subsequently export to Russia.

5. As further detailed herein, funds for these illicit transactions are obtained from the various Russian purchasers, which are initially deposited into one of the defendants' primary Russia-based accounts. Disbursements for purchases were made from that primary Russian account through one or more foreign accounts held by "shell" corporations in the British Virgin Islands ("BVI"), Latvia, Marshall Islands, Panama, Ireland, England, United Arab Emirates, and Belize, and ultimately into one of the defendants' U.S.-based accounts. The defendants transferred monies from the U.S. to Russia in the same fashion. The defendants' creation and use of dozens of shell companies was intended to conceal the true sources of funds in Russia, as well as the identities of the various Russian defense contracting firms who were receiving U.S. electronics components.

Financial Records

6. Documents seized by FBI personnel pursuant to a court-authorized search warrant for an e-mail account used by defendant Brazhnikov included a computer-generated spreadsheet. This spreadsheet contained accounting records for at least 28 separate bank accounts in four different countries (U.S., Russia, Germany, and Cyprus) over which accounts defendant Brazhnikov had direct access and/or control. As explained further below, from in or about 2010 through the present, these accounts have been consistently funded by incoming wire transfers from over 50 different overseas shell corporations.

7. According to FBI analysis, from July 2010 to February 2014, approximately $65,000,000 in wire transfers passed between the 28 accounts and the foreign shell companies. Upon receipt of the wire transfers to the defendants' U.S.-based accounts, banking records show that the defendants routinely made purchases of U.S.-based electronic components for subsequent export to Russia.

8. Significantly, one of the Russian bank accounts (hereinafter, the "Funding Account") has been identified as the primary account from which each of the wire transfers were initiated through the overseas shell companies to the defendants' U.S.-based accounts in 2013. Seized accounting records indicate that during the 2013 fiscal year, over $15,000,000 was wire transferred from the Funding Account to the shell companies. Each of the wire transfers sent from the Funding Account to a given shell

company corresponded to a subsequent wire transfer from the shell company to one of the defendants' business accounts in New Jersey. These records show that the Funding Account is the primary funding and operations account for the financial network the defendants used to conduct their illicit export activities.

9. Further analysis of the spreadsheet and banking records has revealed that deposits into the Funding Account came from multiple sources, including numerous Russian businesses that are authorized to supply electronic components and parts to the Ministry of Defense of the Russian Federation and the Federal Security Service of the Russian Federation (the "FSB"). Other Russian companies making deposits into the Funding Account were involved in the design of nuclear warheads, as well as nuclear weapons strategic and tactical platforms.

10. Seized documents and banking records[3] have revealed the following partial list of at least fourteen known entities that have made significant deposits to the Funding Account, and that have been confirmed as authorized and/or licensed contractors for the Russian military and intelligence services:

a. Imotek: A Russian company authorized to supply parts to the Ministry of Defense of the Russian Federation;
b. VNIIA: Also known as "All Russia Research Institute of Automatics," a Russian institute involved in the development of nuclear weapons for strategic and tactical platforms and firing and neutron initiation systems for nuclear weapons;
c. VNIITF: Russia's second nuclear warhead design institute;
d. Zao Atlas-Kard: A Russian company authorized to supply parts to the FSB;
e. Zao Besant: A Russian company authorized to supply parts to the FSB;
f. Zao Protection Group Jutta: A Russian company authorized to supply parts to the FSB;
g. OAO Scientific and Production Association: A Russian company authorized to supply parts to the FSB;
h. OAO Instrument Plant Tensor: A Russian company authorized to supply parts to the FSB;
i. OOO Ancud: A Russian company authorized to supply parts to the FSB;
j. FGUP Eleron: A Russian company authorized to supply parts to the FSB;
k. OOO O.P.T.: A Russian company authorized to supply parts to the FSB;
l. Avionika VPK: A Russian company authorized to supply parts to the Ministry of Defense of the Russian Federation;

---

[3] Accounting records and other documents seized in this case contained both English and Russian language notations. The names of the Russian companies used in this affidavit have been translated from Russian to English.

m. CTU STC: A Russian manufacturer of vehicles, antennas, tracking devices, and communication equipment for the Ministry of Defense of the Russian Federation and the FSB; and

n. VEKTOR: A Russian company with licenses from the FSB to provide components for the communication networks of Russian nuclear facilities.

11. As stated, analysis of the Funding Account indicates that over $15,000,000 was wire-transferred from this account to the shell companies in 2013 alone. As monies were wire-transferred from the Funding Account to a given shell company, a subsequent wire transfer was found from the shell company to one of the Subjects' export business accounts in New Jersey.

12. For example, on or about December 18, 2013, the Funding Account received a deposit of approximately $188,500 from Avionika VPK, a Russian-based supplier of electronics for the Russian military. On or about December 20, 2013, one of Zond-R's N.J.-based accounts received a deposit in the same amount from a shell company identified as Moriksen AG, indicating that the Funding Account was utilized by the Subjects to secretly send funds from Russia to the U.S. to facilitate the purchase and export of goods for a Russian company licensed to supply goods to the Russian military.

13. Similarly, in or about January 2013, the Funding Account received approximately $350,000 by Imotek, a licensed supplier of electronics parts for the Russian military. On or about February 13, 2013, the Funding Account wire-transferred $250,000.00 to Smoky Hills S.A., a shell company located in the Marshall Islands. Bank records indicate that on or about February 13, 2013, one of the defendants' NJ bank accounts received a wire transfer from Smoky Hill S.A. in the amount of approximately $250,000.00. The defendants then utilized funds in that account to make subsequent purchases of electronics parts, which were then exported to a Moscow address controlled by the defendants' Russia-based conspirators.

14. Further, the Funding Account was funded over two hundred times in 2013, for a total of approximately $710,716, by CTU STC, a licensed supplier of electronics parts for the Russian military and FSB. A review of the Funding Account has revealed that CTU STC funds were dispersed by the defendants through shell companies located worldwide to the defendants' bank accounts in New Jersey, and that these funds were used to make subsequent purchases of electronics components. For example, on or about March 14, 2013, a shell company identified as Pevoni Holdings LTD ("Pevoni"), located in Tortola, BVI, received a wire transfer in the amount of $150,000 from the Funding Account. Subsequently, one of the defendants' NJ bank accounts received a wire transfer from Pevoni in the same amount. Thereafter, from on or about March 15, 2013, through on or about March 26, 2013, the defendants used the same NJ bank account to order electronics components from two U.S. electronics vendors, totaling approximately $124,129. Similarly, on or about March 20, 2013, a shell company identified as Lentar, Ltd. ("Lentar"), located in Belize City, Belize, received a wire transfer in the amount of approximately $248,000 from the Funding Account. Subsequently, one of the

defendants' NJ bank accounts received a wire transfer from Lentar in the same amount. Thereafter, from on or about March 26, 2013, through on or about April 30, 2013, the defendants used the same NJ bank account to order electronics components from a U.S. electronics vendor totaling $240,623.

15. Additionally, FBI agents have analyzed the records of nine export business accounts believed to be owned, operated or controlled by defendant Brazhnikov and his conspirators, as well as nine personal bank accounts belonging to defendant Brazhnikov. The records covered the period from on or about July 1, 2010, through on or about April 16, 2014. The primary source of funding for all nine business accounts can be traced, directly or indirectly, to the approximately $65,000,000 in wire transfers received from the overseas shell companies.

16. As stated, the Subjects used the funding from the shell companies to purchase millions of dollars of electronic components, electronic parts, and related items from U.S. manufacturers and U.S. distributors, many of which were subsequently exported to Russia at fraudulently diminished values, as further described below.

Illegal Export Activities

17. Over approximately the last four years, law enforcement agents have identified approximately 1,923 separate export shipments originated by the defendants in the U.S. The majority of these overseas shipments were facilitated through a shipping company located in Melville, NY (hereinafter, the "SC"). Significantly, of the identified exports shipped in this timeframe, law enforcement officers have been unable to identify a single corresponding EEI form for an SC shipment of an export originated by the defendants.

18. Presumably, the absence of EEI forms for those shipments would indicate the vast majority of the defendants' exports during this timeframe would have had a value of less than $2,500. However, agents have discovered numerous occasions where the defendants knowingly falsified shipping documents to devalue the true worth of their exports. Examples of the defendants' attempts to conceal their ongoing illicit procurement activities are further described below.

19. Law enforcement officers have obtained and reviewed numerous invoices for purchases made by the defendants from a semiconductor manufacturer located in Newbury Port, Massachusetts (hereinafter, "SM"). Specifically, on or about March 4, 2013, records reveal that the defendants purchased three SM microchips containing part number CY7C253KV18-500BZC (the "Microchips"), for a total price of $1,326.99. The defendants' purchase of the Microchips was funded through a credit card in defendant Brazhnikov's name, and the invoice directed that SM ship the items to the NJ Export Companies.

20. Agents subsequently obtained a shipping invoice from SC, dated March 6, 2013, containing the details of a shipment sent from the defendants to an address in Moscow,

under the attention of "Siminovsky Val 12/66," which has been identified as one of the twelve shell addresses controlled by the defendants. The packing list for the shipment contained a line item for the Microchips with a listed value of $5.15 total (or approximately 0.38% of the parts' actual value based on information obtained via open source law enforcement databases). The shipment contained additional line item entries for other electronics components, and the defendants prescribed a total value of $154.45 for all of the goods contained in the shipment.

21. A further review of the additional items contained in the March 6, 2013 shipment, however, revealed similar devaluation of the true cost of the items contained therein. In fact, every other item listed in that shipment was devalued by the same 0.38% factor. Accordingly, law enforcement agents have concluded that the true value of the electronics components contained in the March 6, 2013 shipment was approximately $39,000. Significantly, no EEI form accompanied this shipment, in violation of U.S. export laws.

22. Additional invoices and shipping documents recovered from SM and SC, respectively, reveal similarly illicit purchase and export activity. Specifically, on or about March 15, 2013, records reveal that the defendants purchased quantities of two more SM parts for a total price of $477.90. The defendants' purchase of these parts was funded through a credit card in defendant Brazhnikov's name, and the invoice directed that SM ship the items to the NJ Export Companies.

23. Law enforcement officers subsequently obtained a shipping invoice from SC, dated March 21, 2013, containing the details of a shipment sent from the defendants to a recipient purportedly in Finland. The packing list for the shipment contained line items for each of the aforementioned SM parts with a listed value of $7.99 total (or approximately 1.67% of the parts' actual value, based on information obtained via open source law enforcement databases). The shipment contained additional line item entries for other electronics components, and the defendants listed a total value of $1,845.76 for all of the goods in the shipment.

24. A further review of the additional items contained in the March 21, 2013 shipment revealed similar devaluation of the true cost of the items contained therein. In fact, according to a review of open source pricing databases, every other item listed in that shipment was devalued by the same 1.67% factor. Accordingly, law enforcement agents have concluded that the true value of the electronics components contained in the March 21, 2013 shipment was approximately $110,000. Significantly, no EEI form accompanied this shipment, in violation of U.S. export laws.

25. The transactions identified are indicative of the defendants' pervasive efforts to intentionally devalue exports in order to evade the necessity of filing an EEI form. By secreting the value of the electronic components they export, the defendants are able to conceal the true scope of their unlawful venture.

FORFEITURE ALLEGATION

The Complaint alleges the following for the purpose of noticing forfeiture pursuant to Title 18, United States Code, Section 982.

As the result of committing one or more of the money laundering offenses in violation of Title 18, United States Code, Section 1956, alleged in the criminal complaint, defendant shall forfeit to the United States pursuant to Title 18, United States Code, Section 982, all property, real and personal, involved in the money laundering offense(s) and all property traceable to such property, including but not limited to the following:

1. REAL PROPERTY

a) All that lot or parcel of land, together with its buildings, appurtenances, improvements, fixtures, attachments and easements, located at 177 Longwood Drive, Unit 177, Oak Knoll Townhouses, Manalapan, New Jersey 07726-3845, more particularly described as: Block 1438, Lot C17-7, Assessor's Parcel No. 28-01438-0000-00001-0000-C17-7, in the Town of Manalapan, Monmouth County, New Jersey, being the same property that was described in a deed recorded as Instrument No. 2006078024 in Book 8565, Page 5411. The current record title holders of this property are Alexander Brazhnikov, Zhanna Polonskaya & Alexandre Brajnikov.

b) All that lot or parcel of land, together with its buildings, appurtenances, improvements, fixtures, attachments and easements, located at 234 Central Avenue, Mountainside, New Jersey 07092-1950, more particularly described as: Block 5.T, Lot 65, in the Borough of Mountainside, Union County, New Jersey, being the same property that was described in a grant deed recorded as Instrument No. 227337 in Book 5880, Page 619. The current record title holders of this property are Alexander Brazhnikov and Zhanna Polonskaya.

2. BANK ACCOUNT(S)

a) Up to a total of $2,000,000.00, contained in account number CY29005004820004820731718301 held in the name of Alexander Brazhnikov at Hellenic Bank Public Company, Ltd., Nicosia, Cyprus.

b) Up to a total of $1,880,000.00 in Sberbank Of Russia's interbank or correspondent bank account numbers 0004403077 and 0004169401, held at Deustche Bank Trust Company Americas; and/or account number 8900057610 held at The Bank of New York Mellon; or any other correspondent accounts maintained by Sberbank of Russia at JP Morgan Chase Bank, Wells Fargo, or Bank Of America In The United States.

If any of the above-described forfeitable property, as a result of any act or omission of the defendant(s):

(1) cannot be located upon the exercise of due diligence;

(2) has been transferred or sold to, or deposited with, a third person;
(3) has been placed beyond the jurisdiction of the Court;
(4) has been substantially diminished in value; or
(5) has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Section 982(b), to seek forfeiture of any other property of said defendant up to the value of the above forfeitable property.

All in violation of Title 18, United States Code, Sections 982 and 1956.